CRYPTOGRAPHIC DEVICE AND ASSOCIATED METHODS

Abstract of the Disclosure

A cryptographic device includes an input stage receiving an input data block and a key data block made up of a plurality of sub-key data blocks, and generating a plurality of first signals therefrom. An intermediate stage is connected to the input stage and includes a plurality of substitution units. Each substitution unit substitutes data within a respective first signal. A diffuser is connected to the plurality of substitution units for mixing data to generate a diffused signal. An output stage is connected to the intermediate stage for repetitively looping back the diffused signal to the input stage for combination with a next sub-key data block. The output stage provides an output signal for the cryptographic device after the repetitively looping back is complete.